IEICE Transactions on Fundamentals of Electronics,
Communications of Computer Sciences, E84-A(10): 2606-2609

On the Security of Generalization of Threshold Signature and Authenticated Encryption

Tseng, Yuh-Min; JAN, J. K. ; CHIEN, H. Y.

Abstract

In 2000, Wang et al. proposed a new (t, n) threshold signature scheme with (k, l) threshold shared verification. Meanwhile, integrating the idea of message recovery, they also proposed a (t, n) threshold authenticated encryption scheme with (k, l) threshold shared verification. However, this article will show that both proposed schemes are insecure, because any malicious attacker can obtain the group secret keys from two valid threshold signatures. Thus, the attacker may solely forge or verify a threshold signature. An improvement to overcome the attacks is proposed.